Reg. No. | | | | | | | | | | | | |

Question Paper Code : 27417

5 Year M.Sc. DEGREE EXAMINATION, MAY/JUNE 2016

Ninth Semester

Computer Technology

XCS 593 / 10677 SW 903 – NETWORK SECURITY

(Common to 5 Year M.Sc. Software Engineering and 5 Year M.Sc. – Information Technology)

(Regulations 2003/2010)

Time : Three Hours **Maximum : 100 Marks**

Answer ALL questions.

PART – A (10 × 2 = 20 Marks)

1. What are the key principles of security ?
2. What are replay attacks ? Give an example.
3. Give any three approaches for attacking the RSA algorithm.
4. What are the problems that are associated with direct digital signatures ?
5. What is Off-lien and On-line password guessing ?
6. What is meant by Eavesdropping?
7. Mention the need of KDCs.
8. Name any four functions of Firewalls.
9. List any five security features desirable in E-mail.
10. What is meant by HTTP digest authentication ?

PART – B (5 × 16 = 80 Marks)

11. (a) Elaborate on the passive and active attacks with examples.

OR

(b) Explain the steps of DES algorithm.

12. (a) (i) List the steps in DSS algorithm. **(10)**

(ii) Write short note on modular exponentiation. **(6)**

OR

(b) (i) Discuss in detail Public Key Cryptography standard. **(12)**

(ii) Can the private key operations in RSA optimized ? Justify. **(4)**

13. (a) (i) Discuss in detail about the merits of add nets based authentication over password based authentication. **(8)**

(ii) Explain the various roles of trusted intermediaries with an illustration. **(8)**

OR

(b) (i) Write short notes on :

(1) Eavesdropping **(4)**

(2) Authentication tokens **(4)**

(ii) Compare and Contrast the various cryptographic authentication protocols available. **(8)**

14. (a) Explain the different types of Firewalls. **(16)**

OR

(b) (i) Describe the IP security architecture. **(8)**

(ii) Explain the Kerberos architecture. **(8)**

15. (a) Explain the Message Integrity and Non-Repudiation.

OR

(b) How does fire-wall protect an organization ? Explain various types of fire-walls.